UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

v.

JOSEPH ZANG, et al.,

Defendants.

Case No. 1:12-cv-629

Dlott, J.
Bowman, M.J.

REPORT AND RECOMMENDATION

The above-captioned case, initiated by Plaintiff Javier Luis ("Luis") *pro se* and *in forma pauperis* more than six years ago in Florida, has a lengthy procedural history. After this Court granted a motion to dismiss and entered judgment for Defendant Awareness Technologies, Inc. ("Awareness"), Plaintiff successfully appealed to the Sixth Circuit, which reversed and remanded for further development of the record. *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016).

Following a period of discovery, Awareness filed a motion for summary judgment. (Doc. 213). For the following reasons, the undersigned now recommends granting Defendant's motion.

I. Background

The parties agree that the undersigned's prior Report and Recommendation ("R&R", see Doc. 196) "accurately and exhaustively sets out a procedural history" of this case. (Doc. 213 at 2; Doc 219 at 1). For the convenience of the Court, that history is restated in part.

Plaintiff's claims arise out of divorce proceedings between Joseph and Catherine

Zang in the Hamilton County Ohio Court of Common Pleas. During the course of those proceedings, Catherine learned that her now ex-husband had installed audio and video surveillance equipment in the marital residence, and spyware on a home computer.[1] The computer "spyware" was a product called WebWatcher, which was manufactured and marketed by Awareness.[2] Once installed, WebWatcher allegedly captured electronic communications such as emails and instant messages ("IMs") in real time, and forwarded those communications to servers maintained by Awareness in California, where they were stored for later review and access by WebWatcher users such as Joseph Zang. During his divorce proceedings in state court, Joseph produced emails and messages between Catherine and Javier Luis, the Plaintiff herein, that Joseph allegedly obtained through his use of the WebWatcher product.

Catherine and others impacted by the installation of WebWatcher (though not Luis) responded by filing suit in this Court against multiple corporate and individual defendants, asserting claims under the federal Wiretap Act as well as claims under state law. *See Catherine Zang, et al. v. Joseph Zang, et al*., Case No. 1:11-cv-884. Rather than joining Case No. 1:11-cv-884, Plaintiff Luis, who lives in Florida, filed his own cases against many of the same defendants in Florida state and federal courts.[3] Eventually, Plaintiff's cases were consolidated into one, and on August 20, 2012, the United States District Court for the Middle District of Florida transferred Luis's federal case to this Court, where it was further consolidated for pretrial proceedings with Lead

[1]Importantly, the claims in this case are limited to the installation of WebWatcher on a single desktop home computer, not the installation of secret cameras or recording devices.
[2]Spyware is used for many reasons, including by law enforcement. *See, e.g. State v. Dellas*, 2011 WL 2636996 (N.J. App. July 7, 2011)(affirming conviction on probation violation based upon sex offender's failure to install WebWatcher as directed).
[3]Plaintiff first filed a complaint in state court in Florida on December 16, 2011, before filing a federal case on March 8, 2012. (Doc. 187 at 1-2).

Case No. 11-cv-884. However, all claims and parties in Case No. 1:11-cv-884 were later dismissed and that case was closed, leaving the above-captioned case to stand alone. At this point in the proceedings, the only claims that remain are those that Plaintiff Luis asserts against Defendant Awareness.

In 2012, Defendant Awareness moved to dismiss, for failure to state a claim, the claims asserted in a prior version of Plaintiff's complaint. (Docs. 68, 77). The undersigned recommended granting that motion in an R&R that was adopted by the Court. (Docs. 109, 162). On appeal, the Sixth Circuit Court of Appeals reversed.

The Sixth Circuit held that Plaintiff had alleged sufficient facts in his July 20, 2012 pleading to support two federal claims against Defendant Awareness under the Wiretap Act, as well as two related state court claims. Specifically, the appellate court determined that Plaintiff had adequately alleged that "Awareness intentionally 'intercepted' Luis's electronic communications in violation of 18 U.S.C. § 2511," that Awareness further "violated 18 U.S.C. §2512…by manufacturing, marketing, selling, and operating a device that Awareness knew or had reason to know was to be used primarily for the surreptitious interception of electronic communications," and that "Awareness violated Ohio state law by (1) intercepting and using his electronic communications within the meaning of Ohio's Wiretap Act, and (2) invading his privacy within the meaning of the common-law tort." *Zang*, 833 F.3d at 625.

Following remand, this Court set new pretrial deadlines, including a new deadline by which Plaintiff was permitted to file a motion to further amend his complaint.[4] Plaintiff filed two untimely motions to amend, (Docs. 187, 189), which were nevertheless

[4]Plaintiff previously had amended his complaint multiple times. (*See generally* Doc. 196, at pp 3-7, recounting the history of amendments; *see also, generally*, Docs. 1, 12, 14, 39, 121, 186).

considered “in the interests of justice.” (Doc. 196 at 9, n.8). Ultimately, the Court denied most of the proposed amendments, but permitted Plaintiff to expand upon existing claims against Defendant Awareness. (Doc. 196 at 16). Plaintiff’s last amended complaint was filed on March 28, 2017, and supersedes all prior versions of Plaintiff’s complaint against Defendant Awareness Technologies, Inc. (Doc. 195). The deadline for completion of fact discovery expired on May 1, 2017, and the expert discovery deadline expired on November 30, 2017. (Docs. 177, 179, 181). Defendant filed its motion for summary judgment on December 28, 2017. (Doc. 213).

II. Analysis of Pending Motion for Summary Judgment

A. Standard of Review

In a motion for summary judgment, a court must view “the facts and any inferences that can be drawn from those facts…the light most favorable to the nonmoving party.” *Keweenaw Bay Indian Comm. v. Rising*, 477 F.3d 881, 886 (6th Cir. 2007) (internal quotation marks omitted). “Summary judgment is only appropriate ‘if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law.’ ” *Id*. (quoting Fed.R.Civ.P. 56(c)) (internal quotation marks omitted). “Weighing of the evidence or making credibility determinations are prohibited at summary judgment - rather, all facts must be viewed in the light most favorable to the non-moving party.” *Id.*

The requirement that facts be construed in the light most favorable to the Plaintiff, however, does not mean that the court must find a factual dispute where record evidence contradicts Plaintiff's wholly unsupported allegations. If a moving party has

carried its initial burden of showing that no genuine issues of material fact remain in dispute, the burden shifts to the non-moving party to present specific facts demonstrating a genuine issue for trial. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986). "The 'mere possibility' of a factual dispute is not enough." *Mitchell v. Toledo Hosp.*, 964 F.2d 577, 582 (6th Cir. 1992) (citing *Gregg v. Allen-Bradley Co.*, 801 F.2d 859, 863 (6th Cir. 1986)). In order to defeat the motion for summary judgment, the non-moving party must present probative evidence that supports its complaint. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249-50 (1986). Although reasonable inferences must be drawn in favor of the opposing party, *see Matsushita*, 475 U.S. at 587, inferences are not to be drawn out of thin air. To demonstrate a genuine issue, the opposing party "must do more than simply show that there is some metaphysical doubt as to the material facts.... Where the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no 'genuine issue for trial.' " *Id.*, 475 U.S. at 586-587 (citation omitted).

To the extent that Awareness has shown that Luis lacks evidence on an essential element of his claim, the burden shifts to Luis to set forth "specific facts showing that there is a genuine issue for trial." *Matsushita*, 475 U.S. at 587. At this point, Luis may not rely solely on his subjective beliefs or opinions. *Arendale v. City of Memphis*, 519 F.3d 587, 601 (6th Cir. 2008). He may not simply allude to unspecified records that he believes present some issue for trial, or show only that some hypothetical doubt exists as to the facts, *Matsushita*, 475 U.S. at 586. Rather, Luis must cite to specific evidence of record. Other than expressing general disagreement, however, Plaintiff here has failed to comply with Rule 56 by citing to any "particular" evidence of record to dispute

the facts set forth by Awareness. “The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff.” *Copeland v. Machulis*, 57 F.3d 476, 479 (6th Cir. 1995). Based on the relevant standards, Awareness is entitled to judgment as a matter of law.

B. Threshold Question of Standing and Subject Matter Jurisdiction

Based on the allegations of Plaintiff’s complaint, both this Court and the Sixth Circuit determined that Plaintiff Luis had “adequately alleged facts supporting an inference that **he** is a “person whose ... electronic communication [was] intercepted ... in violation” of the Wiretap Act.” *Zang*, 833 F.3d at 635 (emphasis added).

However, the developed record now presents a serious question concerning Plaintiff’s standing to bring any civil claim under 18 U.S.C. § 2520, as well as his standing to bring the two state law claims. The issue of standing is a threshold issue, and is appropriate to re-examine in this instance because it goes to the Court’s subject matter jurisdiction. *See Bench Billboard Co. v. City of Cincinnati*, 675 F.3d 974, 983 (6th Cir. 2012); *see also generally Steel Co. v. Citizens for a Better Environment,* 523 U.S. 83, 95, 118 S.Ct. 1003 (1998)(holding that reviewing courts should raise issue of standing *sua sponte* where lower court has erroneously assumed its existence); *see also United States v. Corrick,* 298 U.S. 435, 440, 56 S.Ct. 829 (1936).

Fundamentally, Defendant’s unrebutted evidence shows that WebWatcher captured only emails or instant messages that had been fully “delivered” to Catherine Zang on the Zang computer. (Doc. 217. Affidavit of CEO Miller). Thus, even if Plaintiff authored those messages, they were captured only after he had relinquished his

possession and control by "sending" them to the Zang computer. The provision of the Wiretap Act that allows civil suit for transgressions of the criminal provisions of 18 U.S.C. §§ 2511 and 2512 is set forth at 18 U.S.C. § 2520. The express language permits suit only by the "person whose…electronic communication is intercepted, disclosed, or intentionally used." *Id.* The possessive adjective "whose," which modifies "communication," implies ownership, or at least possession or control. On the facts presented, there is no evidence that WebWatcher "intercepted, disclosed, or intentionally used" any "electronic communication," much less any form of communication in *Luis*'s possession or control. The undersigned would conclude, therefore, that Plaintiff lacks standing to bring any of his claims under the Wiretap Act or Ohio's parallel statutes.

For similar reasons, and as more fully discussed below, the undersigned would find that Plaintiff lacks standing to bring an invasion of privacy claim under Ohio law. No Ohio authority appears to support imbuing the sender of the allegedly "private" message (Luis) with any greater expectation of privacy than would be possessed by the recipient (non-party Catherine Zang), whose messages were copied in this case. To the contrary, significant case law supports a conclusion that as the sender of an electronic message, Luis had no "reasonable" expectation of privacy once his messages were actually "sent." *See United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997)("[A]n e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received."); *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)("[I]f a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery…even though the sender may have

instructed the recipient to keep the letters private."); *cf. United States v. Dunning*, 312 F.3d 528, 531 (1st Cir. 2002).

However, mindful that the issue of standing has not been briefed, and that this case is proceeding on remand, the undersigned will assume the possibility of standing and proceed to evaluate the remainder of Plaintiff's claims.

C. Defendant's Unrebutted Evidence Requires Judgment in Its Favor

1. Awareness is Entitled to Judgment on Plaintiff's §2511 Claim

In Count I of his last amended complaint, Plaintiff alleges that Awareness violated 18 U.S.C. §2511 of the Wiretap Act by "intercepting" his communications. (Doc. 195). The cited provision criminalizes the following conduct:

> **(**1) Except as otherwise specifically provided in this chapter any person who--
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication… shall be punished [by a fine or by imprisonment.]

18 U.S.C. § 2511(1)(a). As stated, the Wiretap Act provides for a private civil cause of action for those who are victimized:

> (a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a).

Reviewing a prior version of Plaintiff's complaint, the Sixth Circuit held that Plaintiff had adequately alleged that Awareness itself, and not only Joseph Zang through the use of WebWatcher, had "intercepted" Plaintiff Luis's communications. In reaching that conclusion, the Sixth Circuit first defined - as a matter of first impression -

precisely what Plaintiff would be required to prove at trial in order to demonstrate that Awareness had violated 18 U.S.C. §2511.

Relying on case law from other circuits, the appellate court held that Plaintiff must prove that WebWatcher caused a "contemporaneous" capture or "intercept" of his "electronic communications." *Id*., 833 F.3d at 629. The court drew a distinction between the type of "electronic communications" that are subject to "intercept" under 18 U.S.C. §2511, and "electronic storage," explaining that the distinction "is not an accident of statutory drafting," but instead was intended by Congress to differentiate "between communications in transit and communications in storage," the latter of which are governed by entirely separate statutory provisions contained in Title II of the Electronic Communications Privacy Act. *Id.* at 628.[5] Stressing the differences between the statutory definitions of "electronic communications" and "electronic storage," the appellate court unequivocally held that the term "intercept" in § 2511 "applies solely to the transfer of electronic signals" and not "to the acquisition of electronic signals that are no longer being transferred." *Id.* at 627. Further explaining what is meant by the contemporaneity requirement, the court stated: "Once the transmission of the communication has ended, the communication ceases to be a communication at all…[and] instead becomes part of 'electronic storage.'" *Id.* at 628. In other words, the Sixth Circuit confirmed that §2511 does not apply to email or IMs that reside in "electronic storage," and that the interception must catch the transmitted communication

[5]After remand, Plaintiff moved to amend his complaint to include additional claims that Awareness and others also violated provisions of the Stored Communications Act ("SCA"), see 18 U.S.C. §2701. The SCA generally provides fewer protections to "stored" information than to information intercepted during the "transfer" of the electronic data. However, the Court denied Plaintiff's motion to expand his claims on multiple grounds. (*See* Doc. 196 at 18-19, adopted at Doc. 210).

"'in flight' before the communication comes to rest and ceases to be a communication." *Id.* at 628-629 (internal citation omitted, emphasis added).

Despite limiting the application of §2511 to "signals" during their transmission, the Sixth Circuit held that Luis had sufficiently *alleged* that WebWatcher "contemporaneously" captured Luis's emails and IMs while they were still "in flight," because: (1) his complaint specifically alleged that *Awareness itself* intercepted Luis's communications using WebWatcher; (2) he attached, as part of the amended complaint at issue, three pages of marketing materials that described the features of WebWatcher; and (3) he specifically referred to those marketing materials when describing the way in which Awareness's "device" operates.[6] *Id*. at 630 (citing to prior complaint, Doc. 39).

Based on Plaintiff's prior allegations, the appellate court hypothesized that:

> If a WebWatcher user can in fact review another person's communications in near real time, then WebWatcher must be acquiring the communications and transferring them to Awareness's servers as soon as the communications are sent. The program, in other words, does not wait for the communications to be stored; instead, the program as described captures and reroutes the communications so that a WebWatcher user can review the communications at nearly the same time as they are being transmitted.

Id. at 631.[7] The court pointed out that a statement in the marketing materials indicated that "[e]ven if a document is never even saved, WebWatcher still records it," and construed that statement as an indication that Plaintiff was alleging that "the product

[6]Awareness has not challenged the premise that WebWatcher (and/or the servers maintained by Awareness) constitute an "electronic device" for purposes of the statute. At the same time, there is no dispute that WebWatcher has no physical form like a traditional physical wiretap, but instead is comprised of software, or computer code.

[7]The appellate court's suggestion, based upon the rapidity with which the re-transmission occurred ("in near real time"), that WebWatcher "must" be acquiring the signals "in flight" could be read as implying that any blink-of-an-eye transmission would be incompatible with the acquisition of information from electronic storage. However, read as a whole, the Sixth Circuit's opinion clarifies that regardless of the speed with which technology can transmit a signal, the crux of whether an "intercept" occurs depends on whether the "device" (WebWatcher) transmits the information from the "electronic storage" of a computer, or whether it employs other means to accomplish the rare capture of a signal still "in flight."

records the communications as they are being sent, without regard for whether a copy is ever placed in the storage of the affected computer." *Id.* To that extent, then, Plaintiff had sufficiently alleged that his IMs and emails were "intercepted" while "in flight." *Id.*

Although the CEO of Awareness previously had submitted an affidavit to refute Plaintiff's allegations that WebWatcher caused a "contemporaneous" intercept to occur, the Sixth Circuit rejected that affidavit as premature and procedurally improper in the context of a Rule 12(b)(6) motion to dismiss, where the court must limit itself to a review of the pleadings. Alternatively, the Sixth Circuit noted that even if Awareness's motion were converted to a summary judgment motion, thereby allowing consideration of the affidavit, the affidavit did not "specify how or when WebWatcher actually creates the records" and "therefore does not foreclose the possibility that WebWatcher acquires electronic communications before they come to rest in electronic storage." *Id.* at 633. In other words, the prior affidavit did not rebut the technical *possibility* that "Awareness itself acquires the communications while they are still in transit." *Id.*

Plaintiff's amended complaint after remand more clearly alleges a violation of 18 U.S.C. § 2511, and includes the same marketing materials, along with additional pages of similar materials. (*See* Docs. 195-1 at 41-43, 195-2, and 195-3, *compare with* Doc. 39 at 41-43). Plaintiff alleges that Awareness violated 18 U.S.C. §2511 by intercepting Plaintiff's electronic communications, and that the Defendant "used and delivered to unauthorized third parties thousands" of those communications "instantaneously." (Doc. 195 at ¶¶26-38, 44, 62-70). Plaintiff further alleges that Awareness "itself as a corporation (a) intercepted and (b) stored plaintiff's private communications on its personal servers, (c) used and (d) delivered that information while knowing or having

reason to know the information was gathered illegally." (*Id.* at ¶66). Although the "intercept" of his communications is proscribed by § 2511(1)(a), Plaintiff adds to his current complaint claims that Awareness violated 18 U.S.C. §§2511(1)(c) and (d) when Awareness allegedly "*disclosed* and delivered summaries as well as the entirety of the intercepted communications to their clients" and "used" the intercepted information by delivering it to unauthorized third parties. (Doc. 195 at ¶¶68-69 emphasis original).

In support of summary judgment, Awareness offers a new affidavit prepared by its CEO that states more clearly and unequivocally that neither Awareness nor the WebWatcher software are able to "intercept" electronic communications while in transit in a manner that would violate §2511, but instead, that "any electronic communication accessed by Mr. Zang's use of WebWatcher came from the stored memory of Mr. Zang's own computer." (Doc. 213 at 7, citing Doc. 217 at ¶8). Defendant further points to the absence of any evidence produced by Plaintiff during discovery that would establish any type of "contemporaneous" "intercept" of "electronic communications," as those terms have now been defined by the Sixth Circuit, through the use of WebWatcher. In relevant part, Mr. Miller's affidavit states:

> 8. The WebWatcher product purchased by Joseph Zang must be installed on a specific computer (both physical access and password required) and can only access electronic information that has been stored in the computer's memory. Moreover, WebWatcher is only compatible with specific applications, which means that WebWatcher can only capture data that has already been received and stored in memory of the computer on which WebWatcher is installed, and then only to the extent that the data is transmitted from those specific programs that are supported by WebWatcher. Said another way, WebWatcher sits on the computer and hooks into specific applications, and thus can only access data previously received by those applications on that computer after it has been stored in memory.
>
> 9. WebWatcher does not and cannot access electronic communications

> while the communications are in transmission to the computer on which WebWatcher is installed. It can only access such information after the electronic communication has been received by the computer and put into storage memory.

(Doc. 217, Miller Affidavit at ¶¶8-9).[8]

In response in opposition to Defendant's motion,[9] Plaintiff argues that the issue of whether Awareness "intercepted" Plaintiff's communications while "in flight" has already been decided both by this Court and by the Sixth Circuit Court of Appeals, and therefore is no longer a material fact in issue. Plaintiff is mistaken. The prior opinion of this Court and the controlling opinion of the Court of Appeals both were rendered in the context of a Rule 12 motion to dismiss, and were therefore limited to a determination of whether Plaintiff's complaint *alleged* sufficient facts to state a claim under §2511 of the Wiretap Act. The Sixth Circuit determined only that, based in part on advertising materials attached to the complaint, Plaintiff had adequately alleged that Awareness had violated § 2511, not that Plaintiff had actually proven those allegations and the Defendant's liability. Plaintiff's subsequently amended complaint more clearly articulates the same § 2511 claim, but mere allegations in a complaint are not sufficient to defeat summary judgment.

Plaintiff admits that he "has no formal detailed technical knowledge of the acquisition mechanism," (Doc. 219 at 4), but argues that his § 2511 claim should be submitted to the jury because Awareness "itself has offered no relevant information that

[8]Defendant originally attached an unsigned version of the same affidavit to its motion for summary judgment. (Doc. 213-1). A signed version was filed on January 3, 2018. (Doc. 217).

[9]Plaintiff's response in opposition is comprised of a memorandum entitled "Opposition to Defendant's Motion for Summary Judgment, and Plaintiff's Motion for Leave to Submit Cross Motion for Summary Judgment." (Doc. 219). The latter part of the caption appears to be a mistaken reference to a motion previously denied by this court (Doc. 218). In addition, notwithstanding its caption as a responsive memorandum, the response was mistakenly docketed as an "Affidavit in Opposition re Motion for Summary Judgment" rather than a memorandum.

counters Plaintiff's assertion that the Wiretap Act has been violated." (*Id*.) However, the affidavit attached to Defendant's motion provides relevant, admissible, and uncontroverted evidence that WebWatcher did not cause any contemporaneous intercept of Plaintiff's electronic communications. The affidavit thus shows that Plaintiff lacks evidence on the most critical element of his claim – that there was no "intercept" of his "electronic communications" while the emails and IMs transmitted by Plaintiff to Catherine Zang were still "in flight." That affidavit is neither contradicted by the referenced advertising materials attached to Plaintiff's complaint,[10] nor by any other evidence submitted by the Plaintiff.

The advertising materials previously found to be sufficient to allow for a plausible inference at the pleading stage that Plaintiff had *alleged* contemporaneous interception do not preclude summary judgment at this post-discovery stage of proceedings. The general statements in those marketing materials do not articulate any technical details, and fall well short of creating any genuine issue of fact as to whether WebWatcher intercepted Plaintiff's electronic communications in flight, within the meaning of § 2511, prior to delivery of the emails and/or IMs into the temporary storage or memory of the Zang computer.

Plaintiff additionally argues that the argument by Awareness "that the 'intercept component' is lacking" is based on "ridiculous technicalities that this Court has already dismissed in its R&R." (Doc. 219 at 4) Plaintiff suggests that his own "unfamiliarity with

[10]Plaintiff testified that his primary understanding of how WebWatcher works comes from the advertising materials, but also testified that he does not know whether any of those materials concern the version of WebWatcher that Joseph Zang purchased and installed on his home computer. (Doc. 215, Luis deposition at 40-41). The affidavit filed by Awareness states that the advertising "are from a website (www.awarenesstech.com) that has not been active since 2008, 2 years prior to Zang's purchase" of the version of WebWatcher that is at issue in this case. (Doc. 217 at ¶11). Additional evidence indicates that Joseph Zang purchased WebWatcher from a third party distributor on July 13, 2009.

the process of discovery prevented him from acquiring the information" concerning the timing of the Defendant's alleged "intercept," although he maintains that "it was really not necessary…[because] the timing is irrelevant." (Doc. 219 at 6). Plaintiff contends that the fact that WebWatcher captured both instant messages and emails "*almost* as soon as the message *left or arrived* to the host computer," is sufficient to prove his claim. (Doc. 219 at 6, emphasis added).

Again, Plaintiff is mistaken, both as to the relevance of "timing" (or, more accurately, the mechanism by which WebWatcher retrieves email and instant messages) and as to the burden of proof on summary judgment. The Sixth Circuit's holding - that the requirement that an intercept be contemporaneous and catch a transmission "in flight" - was no mere "technicality," but instead defined the central component of a §2511 claim. Thus, the "when and how" of the alleged "intercept" is critical to the issue of whether an "intercept" occurred.

Finally, although Plaintiff concedes that the emails and messages were retrieved from the Zang computer's "memory" by WebWatcher and not actually "in transit," Plaintiff attempts to distinguish between "temporary" memory or transient storage, referred to as random access memory ("RAM"), and the more permanent type of storage that exists on a hard drive of a computer. He argues that because the "instant messages" that were captured by WebWatcher were not "saved" on the hard drive, but instead remained only in "volatile memory (or RAM)," (Doc. 219 at 6), this Court should find that they were still "intercepted" under the definition of § 2511.

Plaintiff's argument fails as a matter of law. The Sixth Circuit held that for a §2511 violation to occur, the interception must occur when an electronic communication

is still in flight, and not when it has reached *any* form of "electronic storage." Lest there be any doubt, the Sixth Circuit quoted the definition of the term "electronic storage" under the Wiretap Act, which includes "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," (which would include RAM), as well as "(B) any storage of such communication by an electronic communication service for purpose of backup protection of such communication." *Zang*, 833 F.3d at 627 (quoting 18 U.S.C. § 2510(17), emphasis added). In other words, regardless of whether Plaintiff's communications were retrieved from the "temporary" type of storage on the Zang computer that is synonymous with "volatile memory" or "RAM," the fact that WebWatcher retrieved the information from any form of "storage," rather than during the actual "transfer of signs, signals, writing, images, sounds, data" *see id*., quoting 18 U.S.C. §2510(12), dooms Plaintiff's §2511 claim. Defendant is entitled to summary judgment because Plaintiff admittedly has no evidence to contradict the Miller affidavit that the communications were not intercepted but were instead retrieved from a type of electronic storage or memory on the host (Zang) computer.

Plaintiff's reliance on dicta from an unpublished case in the Southern District of New York*, Zaratzian v. Abadir*, 2014 WL 4467919 (S.D.N.Y. Sept. 2, 2014), is also unavailing. In *Zaratzian*,[11] a trial court questioned the reasoning of a line of cases that defined the "contemporaneous" or "in flight" requirement. However, the Sixth Circuit's adoption of the reasoning of those same cases is now settled law. *Accord, U.S. v Steiger,* 318 F.3d 1039, 1048-1050 (11th Cir. 2003)(holding that amendment to Wiretap

[11]Plaintiff erroneously cites to a later opinion from the same case in which the court denied a post-trial motion after the jury rendered a verdict in favor of Plaintiff's ex-husband. *See id*., 2015 WL 5474246 (S.D.N.Y. July 8, 2015).

Act approved of the narrow judicial definition of "intercept" as limited to the "acquisition during 'flight'" for electronic communications, during the "seconds or mili-seconds before which a newly composed message is saved to any temporary location following a second command" despite the fact that "very few seizures of electronic communications from computers will constitute 'interceptions'" (internal quotation omitted, emphasis added)); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994)(holding that search of temporarily stored, unread email that could be deleted once the addressee "called" the electronic bulletin board system ("BBS") to retrieve his/her email, did not violate §2511 because it was not an "intercept" of a communication in transit); *see also U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010)(holding that Defendant's conviction under § 2511 could stand because jury could have found that intercept and copying of email occurred at central server *prior to* receipt of email by target computer, or while the email was still "in flight")[12]; *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp.2d 967, 979 (M.D. Tenn. 2008)("unless an e-mail is actually acquired in its split second transmission over a computer network, it cannot be 'intercepted' as that term is reasonably understood").

Plaintiff alternatively argues that even if the Defendant wins judgment on his claim under §2511(1)(a), the Court should still permit his claims under 18 U.S.C.

[12]The *Szymuszkiewicz* court went on to hold that it would find a "contemporaneous" interception even if it was the target computer, rather than the server through which the email message was sent, that made the copy of the email and sent it to the Defendant. *Id.* at 706. The Seventh Circuit reasoned that if both the Defendant and the intended recipient of the surreptitiously forwarded email were sitting at their computers at the same time, "they would have received each [email] message with no more than an eyeblink in between," which the court reasoned was sufficiently "contemporaneous" to satisfy §2511. *Id.* However, the *Jackson Games* and *Steiger* decisions, as well as the Sixth Circuit, more definitively rely on the distinct definitions of "electronic communications" and "electronic storage" to hold that once a communication is completed or "comes to rest" on the host computer, even if only in temporary storage, it is no longer a communication capable of being intercepted.

§§2511(1)(c) and (d) to proceed to trial, because those claims "are separate" and do not rely upon "the timing of intercept, or whether it was in intermediate storage or not." (Doc. 219 at 3-4). Contrary to Plaintiff's argument, however, the statutory provisions prohibiting the "use" or "distribution" of intercepted information are entirely dependent on whether an "intercept" occurred, as an intercept is a condition precedent to a violation of either provision. *See* 18 U.S.C. §§2511(1)(c) and (d). Based on the unrebutted evidence that none of Luis's electronic communications (whether emails or IMs) were "intercepted" while still "in flight," Awareness remains entitled to judgment as a matter of law on Plaintiff's alternate theories that the Defendant "intentionally disclose[d]…the contents of any…electronic communication, knowing or having reason to know that the information was obtained through the interception of …electronic communication," or that Defendant "use[d]" the contents of information "obtained through the interception of…electronic communication." *Id.*

2. Defendant is Entitled to Judgment on Plaintiff's §2512 Claim

In addition to his §2511 claim, Plaintiff brings a separate cause of action against Awareness for manufacturing, marketing, selling, and operating a wiretapping device in violation of 18 U.S.C. §2512(1)(b). The relevant provision provides for criminal penalties for any person who intentionally

> manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce

Id. The Sixth Circuit previously held that the allegations in Plaintiff's prior amended complaint "easily support an inference that Awareness manufactures a device 'knowing

or having reason to know' that the device is 'primarily useful for…the surreptitious interception of …electronic communications." Again, Plaintiff's ability to maintain his civil suit falls under 18 U.S.C. § 2520, as a person "whose…electronic communication is intercepted, disclosed, or intentionally used in violation of [the Wiretap Act]." *Zang*, 833 F.3d at 634. In both the prior complaint and the most current version, Plaintiff alleges that Awareness manufactured, marketed, and sold WebWatcher with knowledge that it would be primarily used to illegally "intercept" electronic communications, and that Awareness remained actively "engaged" in the operation of WebWatcher by maintaining the servers on which the allegedly intercepted communications were stored. Although the Sixth Circuit stressed that no cause of action would lie against one who merely possessed a wiretapping device, the court held that suit could lie when a defendant "plays an active role in the use of the relevant device to intercept, disclose, or intentionally use a plaintiff's electronic communications." *Id.* at 637. The majority suggested that the §2511 and § 2512 claims did not necessarily rise and fall together because "even if a jury ultimately concludes that only Zang (and not Awareness) intercepted Luis's communications in violation of § 2511, Awareness might still be liable because it "engaged in" that violation (*see* § 2520) by manufacturing, marketing, selling, and actively operating the device that was used by Zang to conduct the intercept." *Id.* at 639 (emphasis added).

Despite the analytical distinctions between the two claims, however, both claims require proof that an "intercept" of "Luis's communications" by someone using the "device" occurred. Based upon the undisputed evidence that no intercept of electronic communications ever occurred through the use of WebWatcher (whether by Joseph

Zang or by Awareness itself), Awareness cannot be held liable for any "active role" in the non-existent intercept. The Miller affidavit confirms that WebWatcher obtained the emails and IMs only after they had been delivered (fully transmitted) to temporary or permanent storage on the Zang computer on which WebWatcher was installed. Thus, Awareness is entitled to judgment as a matter of law on the § 2512 claim.

3. Defendant is Entitled to Judgment on Ohio Wiretap Law Claim

In Count VII of his most recently amended complaint, Plaintiff alleges a violation of the Ohio Wiretap Act. (Doc. 195 at ¶¶96-99). As the Sixth Circuit previously observed, the Ohio Wiretap Act closely parallels the language of 18 U.S.C. §2511, and uses nearly identical definitions of the term "intercept." *Zang*, 833 F.3d at 640. For the same reasons that the Defendant is entitled to judgment on Plaintiff's federal Wiretap claims based upon the lack of any "intercept" of his "electronic communications" while still "in flight," so too is Defendant entitled to judgment as a matter of law on Plaintiff's parallel state claims. *Accord Nix v. O'Malley*, 160 F.3d 343, 348 (6th Cir. 1998)(interpreting the Ohio Wiretap Act identically to the federal Wiretap Act); *see also State v. Poling*, 160 Ohio Misc. 2d 84, 87-88, 938 N.E.2d 1118 (2010).

4. Defendant is Entitled to Judgment on Breach of Privacy Claim

In Count V, Plaintiff alleges that Awareness committed the tort of "invasion of privacy" along with "conspiracy to commit invasion of privacy." (Doc. 195 at ¶¶89-92). Plaintiff specifically alleges that he "had an objectively reasonable expectation of privacy in the conversations and electronic communications that took place between him and [Catherine Zang]," because the referenced "communications were private, and Plaintiff had a right to keep the content of such conversations private." (Doc. 195 at ¶90). He

generally alleges that Awareness "knowingly, recklessly, or negligently disclosed, exploited, misappropriated and/or engaged in widespread usage of Plaintiff's private data, and obtained private and sensitive information for Defendant's own benefit without plaintiff's knowledge, authorization, or consent." (*Id*. at ¶46). He alleges that Awareness "disclosed private and potentially embarrassing facts to the public that were of no legitimate concern to the public." (*Id*. at ¶90).

As the Sixth Circuit previously explained:

> Prevailing on an intrusion claim requires the plaintiff to show that the defendant caused a "wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." *Welling v. Weinfeld*, 113 Ohio St.3d 464, 866 N.E.2d 1051, 1053 (2007) (quoting *Housh v. Peth*, 165 Ohio St. 35, 133 N.E.2d 340, 343 (1956)). The plaintiff must have a "reasonable expectation of privacy" in the area or subject matter in which the alleged intrusion occurs. *Retuerto v. Berea Moving Storage & Logistics*, 38 N.E.3d 392, 406 (Ohio Ct. App. 2015) (internal quotation marks omitted). This expectation depends on the "totality of the circumstances." *Lazette v. Kulmatycki*, 949 F.Supp.2d 748, 761 (N.D. Ohio 2013).

Zang, 833 F.3d at 642.

The "totality of circumstances" is of utmost importance. With limited exceptions, when an individual fails to keep another's confidence, no civil liability will arise even if the breach of confidence was intentional and against the wishes of the party whose personal and confidential information was shared. As an Ohio court recently explained in discussing the "reasonable" expectation of privacy in the analogous Fourth Amendment context, the constitution "does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides …will not reveal it." *State v. Taylor*, 2016 WL 1734084 (Ohio Ct. App. 4th Dist., April 27, 2016). Likewise, Ohio's civil laws generally protect only certain types of information (i.e., proprietary information such as

trade secrets), or confidential information that is shared through a legally protected relationship such as priest/penitent, attorney/client, or doctor/patient.

The internet age invites additional considerations. As a state court in New York remarked eight years ago:

> In this day of wide dissemination of thoughts and messages through transmissions which are vulnerable to interception and readable by unintended parties, armed with software, spyware, viruses and cookies spreading capacity; the concept of internet privacy is a fallacy upon which no one should rely.

People v. Klapper, 902 N.Y.S.2d 305, 307, 28 Misc.3d 225, 226 (N.Y.City Crim.Ct., 2010). While not all adopt such a pessimistic view of internet privacy concerns, ever-evolving technology - including the ease with which emails may be forwarded and instant messages may be captured and shared - mandates a closer look at what is a "reasonable" expectation of privacy in the digital age.

In addition, courts will consider as part of the totality of the circumstances the relationship of the party who seeks to recover to the information that has been disclosed, separate and apart from the issue of "standing." Thus, the party who possessed the "private" information may have suffered greater damage, or have a stronger interest in recovery, than parties further afield. Here again, the person whose messages were disclosed turns out not to be Luis (since he had already "sent" his messages prior to their retrieval), but Catherine Zang, insofar as it was her information that was retrieved and/or retransmitted by WebWatcher. Plaintiff testified that he was aware that the desktop computer to which he transmitted his messages was located in a home that Catherine shared with her husband. There is no evidence that the computer was locked away in a room to prevent other family members from accessing it.

Once installed, the WebWatcher software operated indiscriminately, and captured from the computer's memory and/or other storage various activity on that computer, including emails sent/received and instant messages. There was no direct "intercept" of any of Luis's messages but only a retrieval and re-transmission of messages that he authored, insofar as they were stored on the Zang computer. Other entities and individuals who sent messages to anyone using the Zang computer at the time WebWatcher was installed would have been equally impacted by the forwarding of their messages to Joseph Zang and/or the Awareness servers. Clearly, however, not every entity or individual who sent an innocuous email or message to or from the impacted Zang computer could present a claim against Awareness for breach of privacy under Ohio law. "[T]he affairs or concerns must be *private* to rise to be actionable as an invasion of privacy." *Lazette v. Kulmatycki*, 949 F.Supp.2d at 760–61. (emphasis added).

Also pertinent to the totality of circumstances, the Miller affidavit offers unrebutted evidence that the WebWatcher product purchased by Joseph Zang required him to install the software on a computer owned by him, and to notify all users of that computer that they were being monitored.[13] (Doc. 217 at ¶6). Joseph Zang was required to agree to those same terms both at the time of installation and on each occasion that he logged into WebWatcher. (*Id.*) A copy of the license agreement and on-line terms and conditions for WebWatcher is attached to the Miller affidavit, and states in relevant part:

> YOU AGREE TO ONLY INSTALL THIS SOFTWARE ON A COMPUTER OR COMPUTERS OWNED BY THE USER. USER ALSO AGREES TO

[13]Plaintiff testified that he does not know whether Joseph Zang actually owned the computer. "I believe it was hers or his or both. I'm not really certain." (Doc. 215, Luis Depo at 28).

> INFORM ANY PERSON(S) WHO USES A COMPUTER WITH THE SOFTWARE INSTALLED OF THE PRESENCE OF THE SOFTWARE. FAILURE TO COMPLY MAY RESULT IN YOU BREAKING STATE AND FEDERAL LAWS.

(Doc. 217 at 5, Exh. 2, capitalization original). On the record presented, Joseph Zang or his agent agreed to the licensing agreement when he installed WebWatcher on the desktop computer located in his marital home.[14]

Last, although the undersigned finds no need to discuss the issue in depth given the extensive analysis of other circumstances, the degree to which the "private" information is disseminated, and the context in which it is published, is often relevant. Thus, a spouse revealing a confidence in a divorce or custody proceeding may not support an intrusion claim as readily as the broader and more public airing of dirty laundry.

Returning to the elements of Plaintiff's claim as defined by the Sixth Circuit, he must prove that: (1) that Defendant Awareness caused (2) a "wrongful intrusion" (3) into Plaintiff's private activities; (3) in an area or subject matter in which his expectation of privacy was "reasonable" and (4) that Awareness caused such intrusion "in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." *Zang*, 833 F.3d at 642. In considering these elements and the totality of circumstances presented, I conclude that Defendant is entitled to judgment as a matter of law because Plaintiff cannot show several critical elements: (1) that Awareness actively did anything to "cause" an intrusion; (2) that any intrusion by Awareness was "wrongful" under Ohio law; (3) that Plaintiff's expectation of privacy was "reasonable"; or (4) that *Plaintiff's* "private" matters were divulged in any manner to

[14]There is some evidence that Joseph's sister assisted him in installing the software.

anyone that would support liability under Ohio law.

a. The Licensing Agreement

Based on the licensing agreement, and other unrebutted facts including that Joseph Zang installed WebWatcher on the impacted computer, the undersigned first concludes that Awareness did nothing to "cause" any "intrusion" that may have occurred. The undersigned finds instructive *Hayes v. SpectorSoft Corp*., 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009), a case in which a suspicious wife surreptitiously installed similar spyware on a laptop computer used predominantly by her husband. Prior to installation, the software required the user/installer to agree to licensing terms like those spelled out in the WebWatcher agreement. Mrs. Hayes clearly violated those terms and did not inform her husband of the software. The husband filed suit against his former wife, her accomplice-sister, and the software manufacturer, alleging violations of Tennessee and federal wiretap laws, as well as miscellaneous state law claims including a claim that the software manufacturer "aided and abetted" an invasion of his privacy. The court granted summary judgment to the software manufacturer, based on evidence that it "did not know Plaintiff's wife and sister were misusing the software," or "who owned or predominantly used the particular computer," or "what consent had been obtained regarding monitoring or installation." *Id.* at 2. The court focused on the defendant's lack of intention to divulge the plaintiff's private communications, as evidenced by the licensing agreement. Relying on the general enforceability of license agreements that require a purchaser to accept terms of use prior to installing and using software, the court held that the defendant "had every right to expect that its software should be used in accordance with the licensing agreement it

provides." *Id.* at *8.

> To hold Defendant liable under the ECPA for Ms. Hayes'…conduct, of which it was unaware and which breached the terms of its licensing agreement, could result in several unintended results…. [N]o authority… holds the public server liable for the …breach of a licensing agreement that enabled the spouse to capture her partner's private electronic communications. This court concludes that any divulgence by SpecterSoft was inadvertent, and thus, it did not have the necessary *mens rea* for liability [under state of federal Wiretap laws].

Id.[15] Although the Plaintiff in *Hayes v. SpectorSoft Corp*. had alleged that the software company also had "aided and abetted" an invasion of privacy under state law, the court concluded that the plaintiff had not created a genuine issue of material fact regarding that claim, because there was no evidence that the company "took an affirmative act that encouraged [the ex-wife] to violate Plaintiff's rights," and in fact, the licensing agreement provided contrary evidence that the company "attempted to protect the rights of persons like Plaintiff by requiring Ms. Davis to accept its licensing terms prior to being allowed to install its software." *Id.* at *9.

a. The Lack of Evidence that the Intrusion was "Wrongful"

Although Plaintiff's complaint alleges conduct akin to intercepting a letter placed in outgoing mail, *before* it is delivered to the recipient, the evidence shows that neither Joseph Zang (nor Awareness, through the installation of WebWatcher) "intercepted" or viewed any emails and messages directly from Plaintiff's computer or as they were being sent. Rather, Joseph and/or Awareness only accessed emails and instant messages that had been placed into "electronic storage" or "delivered" to the Zang desktop computer. The record therefore establishes that the only "intrusion" was into Catherine's email and/or instant message accounts, not into Plaintiff's own computer.

[15]The court alluded to authority relating to the illegal interception of spousal communications under Tennessee law, but Ohio law appears to differ on that issue.

Because Plaintiff cannot prove that any "intercept" occurred of his "electronic communications," he cannot prove that any intrusion was sufficiently "wrongful" to support his claim of invasion of privacy under Ohio law. *Compare Zang*, 833 F.3d at 642 (holding that violation of state and federal wiretap laws would support the "wrongful" element of an invasion of privacy claim).

b. The Allegedly Private Subject Matter of the Intrusion

In his deposition, Plaintiff testified that he first began communicating with Catherine Zang in a Metaphysics "chat room," and that the conversation began with discussion about football playoffs. (Doc. 215, deposition at 13).[16] Plaintiff and Catherine chatted on and off over the course of weeks, and by January 2009,[17] when they first began communicating more regularly, they did not talk about Catherine's marriage. (*Id*. at 16-17). In addition to contact via the Zang desktop computer, Plaintiff and Catherine spoke by phone on nearly a daily basis.[18] (*Id.* at 19-21).

Plaintiff's discovery responses, attached as exhibits to his deposition, fail to identify any information that was "private and potentially embarrassing" that was disclosed by the attorney representing Joseph Zang in divorce proceedings. (*See generally*, Doc. 216-6 at 11-21, answers to Interrogatories 5-8, 11-14, 16)(stating that Plaintiff has "been trying for months to get information" but has been unable to obtain any responsive information and is therefore "unaware of the embarrassing things [lawyer] disclosed, other than what I gathered from the public filing of the plaintiffs in the

[16]Under Rule 56(c)(3), Fed. R. Civ. P., a court "need consider only the cited materials, but it may consider other materials in the record." The undersigned has considered pages of Plaintiff's deposition beyond those cited by Defendant.

[17]In his deposition, Plaintiff first references the year in which he and Catherine Zang began their correspondence as 2010, but he later corrects that response to 2009.

[18]Plaintiff testified that they did not text at that time, since the time period preceded the prevalence of that method of communication. Regardless, Awareness is alleged to have played no surveillance role other than through its product, WebWatcher, installed on the single home computer.

connected cases which had [lawyer] trying to enter the intercepts into evidence [in the state court proceedings]"); *see also* Doc. 216-6 at 23, response to requests for production, stating that Plaintiff does not possess copies of responsive "communications between you and Catherine Zang" beyond any "intercepts" presumed to be in the possession of Awareness, or "copyrighted songs Catherine Zang wrote during her ordeal").

In order to be actionable under Ohio law, the intrusion must be into subject matter that is "private." As discussed, most of Plaintiff's discovery responses and testimony do not suggest that any "private" information was accessed or revealed by Awareness. On the other hand, Plaintiff provided limited testimony that at least some of the conversations had "a sexual component."

> Q. All right. Without going into any detail –
>
> A. Okay.
>
> Q. -- some of your communications with her electronically had some sexual component to it?
>
> A. Yes, uh-huh.
>
> Q Is it your understanding that she was having similar sexual conversations with other men besides you?
>
> A. I believe she was, yeah. In fact, some of the – some of the intercepts that she sent me – and I can't see them here – were not of me, of her.
>
> Q Oh, she sent you some that were between her and other men?
>
> A. Yeah.

(Doc. 219 at 48). Based on this deposition testimony, the undersigned will assume that the subject matter of at least a portion of the messages sent to Catherine Zang and retrieved by WebWatcher were of a sufficiently "private" nature that intrusion into those

conversations could be actionable.[19]

c. Reasonable Expectations of Privacy Between Spouses

As stated, the undersigned finds that Plaintiff – at most – possesses a privacy interest no greater than that possessed by Catherine Zang, the person whose messages were retrieved by Joseph Zang through his use of WebWatcher. Even assuming that Luis enjoyed an expectation of privacy in conversations that contained "a sexual component," and further assuming (despite the lack of supporting authority) that as the sender of the message he retained a privacy interest on par with Catherine's interest, Ohio and other courts clearly afford a lower degree of privacy when ascertaining "reasonable" privacy expectations between spouses or other family members who share a home.[20] Thus, case law suggests that a spouse or child engaged in alleged sexual misconduct has no "reasonable" expectation of privacy when the damning evidence has been discovered in a shared marital home.

Although no Ohio case exists that is directly on point, in *Beaber v. Beaber*, 322 N.E.2d 910 (Ohio Ct. Com. Pl. 1974), ***aff'd*** No. 4187 (Ohio App., 5th Dist., Aug. 4, 1975), a suspicious spouse surreptitiously recorded telephone conversations between his wife and her lover. The Ohio trial court permitted the evidence to be introduced in the divorce and custody proceedings, recognizing an interspousal exception to the Ohio and federal wiretap laws, based on the reasoning of a Fifth Circuit case, *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974). *Id.* at 915. Despite acknowledging the

[19]There is no dispute that Luis and Catherine Zang never met in person until well after their on-line correspondence had been discovered. The cultural implications of "online infidelity" well exceed the scope of this Court's limited legal opinion. *But see generally* Sandi Varnado, *Avatars, Scarlet "A"s, and Adultery in the Technological Age*, 55 Ariz. L. Rev. 371 (Summer 2013)

[20]Even without the added intimacy of a spousal relationship, Ohio recognizes a diminished expectation of privacy in shared space. *See Retuarto*, 38 N.E.3d at 407 (finding no reasonable expectation of privacy where employee shared office space).

subsequent rejection of *Simpson* by the Sixth Circuit, another federal district court later concluded "that the Ohio Supreme Court would likely recognize the existence of an interspousal exception under Ohio Rev. Code §§ 2933.51 and 2933.58, the Ohio Wiretap provisions. *See Potter v. Havlicek*, 2007 WL 539534 at *8 (S.D. Ohio Feb. 14, 2007)(discussing *Beaber*).[21] Although the Sixth Circuit has now repudiated the interpretation of the Wiretap Act adopted in *Potter*, the undersigned finds persuasive the *Potter* court's view that Ohio limits the degree of privacy that is reasonably expected between spouses.

In other cases evaluating the privacy interests between spouses under similar circumstances, courts similarly found no invasion of privacy, either because there is no "reasonable" expectation of privacy where a single computer is used by multiple people in the home, or because of special considerations when the home is occupied by children, or because a spouse (or other family member) is deemed to have given "implied" consent. The case of *White v. White*, 344 N.J. Super. 211, 781 A.2d 85, 90-91 (2001) is illustrative. There, the court held that a spouse's access to e-mail was not "without authorization" and privacy interest was not "reasonable" where family computer was in area of marital residence where the entire family had access to it.

> The crux of the issue is that the intrusion must be "highly offensive to a reasonable person." *Id.* And that conclusion turns on one's reasonable expectation of privacy. A "reasonable person" cannot conclude that an intrusion is "highly offensive" when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy.

White v. White, 781 A.2d 85, 91–92, 344 N.J.Super. 211, 222 (N.J.Super.Ch., 2001). The White court further reasoned:

[21]In *Potter*, the district court held (contrary to the Sixth Circuit's opinion in this case) that a sufficiently contemporaneous intercept had occurred through a suspicious spouse's installation of spyware.

> Can it be said that defendant's activities here are "highly intrusive?" … She was searching for *indicia* that her husband was involved in an extramarital liaison -not an uncommon occurrence in the realm of human experience. Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet, as in *Del Presto, supra?*
>
> Not really.

White, 781 A.2d 85, 92, 344 N.J.Super. 211, 223–24 (N.J.Super.Ch.,2001).

Another Ohio case that confirms the generally lower expectation of privacy between family members of the same household is *State v. Poling*, 938 N.E.2d 1118, 160 Ohio Misc.2d 84, 2010 -Ohio- 5429, ¶ 12 (Ohio Mun., 2010). In *Poling*, a parent accessed her daughter's emails and messages on a shared computer, but the court determined that the parent possessed something akin to "implied consent." Notably, *Poling* cited two cases involving suspicious spouses. *See id*., 938 N.E.2d at 1122–23 (citing *Bailey v. Bailey,* 2008 WL 324156 (E.D. Mich. Feb. 6, 2008)(rejecting Wiretap Act claim brought by an ex-wife against her ex-husband involving key-logging software installed on shared computer, further holding that the SCA protection does not extend to e-mails and messages stored only on plaintiff's personal computer) and *Evans v. Evans*, 169 N.C.App. 358, 610 S.E.2d 264 (2005)(sexually explicit e-mails that wife had sent to physician, offered by husband in divorce action in support of grounds for divorce and in support of denying post separation spousal support to wife, were not illegally intercepted in violation of ECPA, where interception of e-mails was not contemporaneous with transmission; e-mails were stored on and recovered from hard drive of family computer).

Of course, some courts have recognized a higher degree of privacy in "spying spouse" cases. *See Klumb v. Goan*, 884 F. Supp.2d 644 (E.D. Tenn 2012)(upholding

damages against ex-wife who surreptitiously installed spyware under interpretation of state and federal Wiretap Act now rejected by Sixth Circuit). However, many other courts have found no "reasonable" expectation of privacy exists between spouses in the contents of a shared marital computer. *See generally, Zepeda v. Zepeda,* 2001 S.D. 101, 632 N.W.2d 48 (S.D. 2001) (information obtained from keystroke program allowed to show amount of time spent on Internet in proving adultery); *United States v. Politi*, 2003 WL 21078119, at *4 (S.D. Ind. May 1, 2003) (holding that wife had authority to consent to search of computer in husband's home office, and husband had no reasonable expectation of privacy); *State v. Appleby*, 2002 WL 1613716 at **2-4 (Del. Super. Ct., July 18, 2002) (holding that wife had authority to turn hard drive over to police since she and estranged husband comingled and co-owned the computer equipment, and husband had no reasonable expectation of privacy.)[22] The lower cultural expectation of privacy between spouses who share living space also has been recognized in other contexts involving surreptitious surveillance. *See Colon v. Colon*, 2006 WL 2318250 (N.J. Super. Ct. App. Div. 2006) (video surveillance not invasion of privacy as husband had no reasonable expectation of privacy in office next to master bedroom which was used freely by both wife and children).

The moral norms of society help inform the court's judgment of what constitutes a "reasonable" privacy interest under Ohio law. Ultimately, however, this Court sits in

[22]For helpful academic discussions of this topic, *see generally,* Alison G. Turnoff, *Spying Spouses and Their High-Tech Tool*, 96 Ill. B.348, 372 (2008); Jennifer Mitchell, *Sex, Lies, and Spyware: Balancing the Right to Privacy Against the Right to Know in the Marital Relationship*, 9 J.L. & Fam. Studies 171 (2007) (noting that "courts have historically found little (if any) expectation of privacy between spouses," *id.* at 172, and that "because spouses typically have joint ownership of (or at least access to) the home computer, 'marital use of surveillance software falls through a loophole.'" *id.* at 180); Camille Calman, *Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers*, 105 Colum. L. Rev. 2097, 2126 (2005).

judgment only of the legality, and not the morality, of Joseph Zang's installation of WebWatcher on a computer in a home shared by his wife and children. Based upon Ohio law and the totality of the circumstances recounted in this case, Defendant Awareness is entitled to judgment on the invasion of privacy claim as a matter of law.

III. Conclusion and Recommendation

For the reasons discussed above, **IT IS RECOMMENDED THAT** Defendant's motion for summary judgment (Doc. 213) be **GRANTED**, with judgment to be entered in favor of Defendant, and this case to be closed and stricken from the active docket.

s/ Stephanie K. Bowman
Stephanie K. Bowman
United States Magistrate Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

v.

JOSEPH ZANG, et al.,

Defendants.

Case No. 1:12-cv-629

Dlott, J.
Bowman, M.J.

NOTICE

Pursuant to Fed. R. Civ. P. 72(b), any party may serve and file specific, written objections to this Report & Recommendation ("R&R") within **FOURTEEN (14) DAYS** of the filing date of this R&R. That period may be extended further by the Court on timely motion by either side for an extension of time. All objections shall specify the portion(s) of the R&R objected to, and shall be accompanied by a memorandum of law in support of the objections. A party shall respond to an opponent's objections within **FOURTEEN (14) DAYS** after being served with a copy of those objections. Failure to make objections in accordance with this procedure may forfeit rights on appeal. *See Thomas v. Arn,* 474 U.S. 140 (1985); *United States v. Walters,* 638 F.2d 947 (6th Cir. 1981).